RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

FR99/02992

EO

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 08 DEC. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 29 DEC 1998
N° D'ENREGISTREMENT NATIONAL 98 16550
DÉPARTEMENT DE DÉPÔT 75
DATE DE DÉPÔT 29 DEC. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

RINUY, SANTARELLI
14, avenue de la Grande Armée
75017 PARIS

n°du pouvoir permanent — références du correspondant: BIF022088/FR/EP — téléphone: 01 40 55 43 43

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale: ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Dispositif et procédé de protection de données sensibles et machine à affranchir les mettant en oeuvre.

3 DEMANDEUR (S) n° SIREN — code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination — Forme juridique

Nom	Forme juridique
SECAP	Société Anonyme
ASCOM AUTELCA AG	Société de droit Suisse.

Nationalité (s) FRANÇAISE SUISSE

Adresse (s) complète (s) — Pays

Adresse	Pays
21, quai Alfonse Le Gallo, 92100 BOULOGNE-BILLANCOURT, FRANCE.	FRANCE
Worbstrasse 201, CH-3073 Gümlingen SUISSE.	SUISSE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Marc SANTARELLI N°92.1222
RINUY, SANTARELLI

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BIF022088/FR/EP

DIVISION ADMINISTRATIVE DES BREVETS
26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL
9816550

TITRE DE L'INVENTION :
Dispositif et procédé de protection de données sensibles et machine à affranchir les mettant en oeuvre.

LE(S) SOUSSIGNÉ(S)
Société Anonyme SECAP
Société de droit Suisse. ASCOM AUTELCA AG

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

DERY Jean-Marc
2, rue Liouville,
92600 ASNIERES, FRANCE.

L'HÔTE Frédéric
5, square Jean Thébaud,
75015 PARIS, FRANCE.

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

29 Décembre 1998

Bruno QUANTIN N°92.1206
RINUY, SANTARELLI

BA 113/271196

La présente invention se rapporte à un dispositif et à un procédé de protection de données sensibles et à une machine à affranchir les mettant en oeuvre.

Elle s'applique en particulier aux machines à affranchir dotées d'un programme s'exécutant dans un environnement multi-tâches et plus généralement à la protection de données sensibles, représentant par exemple, des sommes d'argent, ou de tâches sensibles manipulant les données sensibles.

Dans un environnement multitâches, chaque tâche peut appeler chaque routine, quelle que soit la sécurité nécessaire sur ladite routine. Dans une machine à affranchir, certaines tâches mettent en œuvre des montants représentant des sommes d'argent. En particulier, les phases d'exploitation d'une machine d'affranchissement ou de recharge utilisent les routines qui manipulent des sommes d'argent.

La mise en oeuvre correcte de chacune de ces tâches doit être garantie. On entend par mise en oeuvre correcte, le fait qu'une tâche s'exécute dans le cadre normal du fonctionnement de la machine. En d'autres termes, l'invention vise à empêcher que des données sensibles ne soient altérées ou modifiées de manière inopportune.

A cet effet, la présente invention vise à ce que au moins une routine agissant sur des données sensibles vérifie l'identité de tâches qui lui font appel.

Ainsi, si une tâche non autorisée tente de faire appel à ladite routine, celle-ci peut limiter son exécution et donc éviter de porter atteinte aux données sensibles considérées.

Selon un premier aspect, la présente invention vise un procédé de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données, caractérisé en ce qu'il comporte, mise en oeuvre par ladite routine, une opération de vérification d'identité de chaque tâche logicielle appelant ladite routine.

Grâce à ces dispositions, si une tâche non autorisée est utilisée pour accéder à ladite routine qui utilise des données sensibles, en vérifiant son identité, cette routine détecte qu'elle n'est pas autorisée et empêche l'accès aux données sensibles considérées.

Dans le cas d'une machine à affranchir, par exemple, les routines concernées comportent la routine d'incrémentation du compteur de montant d'affranchissement consommé et de décrémentation du compteur de montant d'affranchissement restant disponible et la routine d'incrémentation du compteur de nombre d'affranchissement effectués.

Selon des caractéristiques particulières, ladite opération de vérification comporte une opération de lecture d'un identifiant de ladite tâche et une opération de comparaison dudit identifiant, d'une part, et d'identifiants prédéterminés, d'autre part.

Grâce à ces dispositions, toutes les tâches autorisées à mettre en oeuvre la routine en question sont identifiées dans une liste particulière, ce qui facilite la programmation de la routine et la mise à jour de cette programmation.

Selon d'autres caractéristiques particulières, chaque routine agissant sur lesdites données met en oeuvre ladite opération de vérification.

Grâce à ces dispositions, quelle que soit la routine qui tente d'accéder aux données sensibles, la protection offerte par la présente invention est assurée par ladite routine.

Selon un deuxième aspect, la présente invention vise un dispositif de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données, caractérisé en ce qu'il comporte un moyen de vérification

adapté à vérifier l'identité de chaque tâche logicielle appelant ladite routine, le moyen de vérification étant mis en oeuvre par ladite routine.

L'invention vise, aussi, une machine à affranchir, caractérisée en ce qu'elle comporte un dispositif tel que succinctement exposé ci-dessus.

L'invention vise aussi :

- un moyen de stockage d'informations lisible par un ordinateur ou un microprocesseur conservant des instructions d'un programme informatique caractérisé en ce qu'il permet la mise en oeuvre du procédé de l'invention telle que succinctement exposée ci-dessus, et

- un moyen de stockage d'informations amovible, partiellement ou totalement, et lisible par un ordinateur ou un microprocesseur conservant des instructions d'un programme informatique caractérisé en ce qu'il permet la mise en oeuvre du procédé de l'invention telle que succinctement exposée ci-dessus.

Ce dispositif, cette machine à affranchir et ces moyens de stockage présentant les mêmes caractéristiques particulières et les mêmes avantages que le procédé succinctement exposé ci-dessus, ces avantages ne sont pas rappelés ici.

D'autres avantages, buts et caractéristiques ressortiront de la description qui va suivre, faite en regard des dessins annexés dans lesquels :

- les figures 1A et 1B représentent, respectivement en vue de dessus et en élévation, une machine à affranchir mettant en oeuvre le dispositif et le procédé de protection de données objets de la présente invention,

- la figure 2 représente, schématiquement, un circuit électronique incorporé dans la machine à affranchir illustrée en figures 1A et 1B, et

- la figure 3 représente un algorithme de fonctionnement du circuit électronique illustré en figure 2.

La machine à affranchir 1 illustrée sur les dessins (figures 1A et 1B) comporte un dispositif pour imprimer, sur un objet plat tel que la lettre 2, d'une part, une marque d'affranchissement et, éventuellement, une adresse de destination de l'enveloppe.

Pour imprimer la marque d'affranchissement sur l'emplacement normalisé prévu à cet effet, il faut faire passer la lettre 2 dans un couloir 5 que

comporte la machine 1, ce couloir étant délimité par des éléments solidaires du bâti, respectivement un support de glissement 6 qui forme le plafond du couloir 5, une table 7 qui en forme le plancher et une rampe qui en forme une limite latérale, le couloir étant ouvert à l'opposé de cette rampe.

Pour faire passer la lettre 2 dans le couloir 5, on pose la lettre sur la partie de la table 7 qui est en saillie du côté prévu pour l'introduction (côté que l'on voit à gauche en figure 1B) puis on fait rentrer la lettre dans le couloir 5, comme montré en figures 1A et 1B, jusqu'à ce qu'elle soit entraînée par les moyens prévus à cet effet dans la machine 1, l'impression de la marque d'affranchissement s'effectuant automatiquement pendant que la lettre 2 est entraînée dans le couloir 5, la lettre affranchie étant expulsée de la machine à l'autre extrémité du couloir 5 (extrémité que l'on voit à droite en figure 1B).

Pour entraîner la lettre 2, la machine 1 comporte deux galets 9 et 10 passant chacun au travers d'une ouverture de la table 7, et deux contre-galets 12 et 13, respectivement pour le galet 9 et pour le galet 10, passant au travers d'une ouverture du support 6.

Les galets 9 et 10 sont montés à rotation par rapport au bâti de la machine 1, par l'intermédiaire de moyens de suspension 14 montrés schématiquement sur la figure 1B.

Les contre-galets 12 et 13 sont montés à rotation sur le bâti de la machine 1, sans être suspendus par rapport à celui-ci. Un moteur électrique non représenté sert à entraîner en rotation synchrone les contre-galets 12 et 13, par exemple par l'intermédiaire d'une courroie (non représentée) qui tourne autour de trois pignons portés respectivement par le moteur, par le contre-galet 12 et par le contre-galet 13.

Etant donné que les moyens de suspension 14 sollicitent les galets 9 et 10 vers le support 6, et donc vers les contre-galets 12 et 13, les galets 9 et 10 sont entraînés par friction sur les contre-galets 12 et 13, directement ou par l'intermédiaire d'un objet, tel que la lettre 2, en cours de passage dans la machine 1.

La lettre 2, lorsqu'elle est introduite dans le couloir 5 comme montré sur la figure 1B, finit par rencontrer le galet 9 puis le contre-galet 12 qui

l'entraîne dans le sens indiqué sur la figure 1B par la flèche horizontale orientée de gauche à droite. Simultanément, le galet 9 s'abaisse tandis que la lettre 2 s'introduit entre les galets 9 et 12 de sorte que la lettre 2 progresse dans la machine 1 avec sa face à imprimer 4 qui est plaquée et qui glisse contre la surface 17 du support de glissement 6.

Pour imprimer la marque d'affranchissement à l'emplacement normalisé qui lui correspond et/ou l'adresse de destination à l'emplacement normalisé qui lui correspond, la machine 1 comporte des moyens d'impression 19 montrés très schématiquement sur la figures 1A et 1B.

D'une façon générale, les moyens d'impression 19 déposent la marque d'affranchissement pendant que la lettre 2 ou l'objet à affranchir circule dans la machine 1 avec sa face à imprimer qui est plaquée contre la surface 17 du support de glissement 6, les moyens 19 étant situés entre les contre-galets 12 et 13.

Dans l'exemple illustré, les moyens d'impression 19 sont montés directement sur le bâti de la machine, et sont donc fixes par rapport au support de glissement 6.

Afin que les moyens d'impression 19 soient commandés en synchronisme avec l'avancement de l'objet dans la machine, il est prévu un détecteur de présence de l'objet (référencé 110 en figure 2) qui déclenche un processus d'impression se déroulant automatiquement.

Plus précisément, il existe un premier détecteur de présence qui commande la mise en route du moteur (non représenté) lorsqu'un objet commence à être introduit dans la machine 1, et un deuxième détecteur de présence (non représenté) qui déclenche le processus d'impression lorsque l'objet est parvenu à un emplacement prédéterminé.

En figure 2, est représenté un circuit électronique de commande du dispositif tel que présenté en figures 1A et 1B. Ce circuit est illustré sous forme de schéma synoptique et représenté sous référence générale 100. Il comporte, reliés entre eux par un bus d'adresses et de données 102 :

- une unité centrale de traitement 106 ;
- une mémoire vive RAM 104 ;

- une mémoire morte ROM 105 ;
- un port d'entrée sortie 103 servant à recevoir :
  - le poids de l'objet postal à affranchir, et
  - la détection de l'objet postal par chacun des détecteurs (non représentés aux figures)

  et à transmettre :
  - des signaux de commande de moteurs, et

  et, indépendamment du bus 102 :
- des moteurs pas-à-pas 109 ;
- des détecteurs de présence 110 ;
- un écran de visualisation 108 relié au port d'entrée/sortie 103 ;
- une balance 112 reliée au port d'entrée/sortie 103 et fournissant des octets représentatifs du poids d'un objet postal ;
- un clavier 101 relié au port d'entrée/sortie 103 et fournissant des octets représentatifs des touches de clavier successivement utilisées ; et
- un contrôleur d'impression 120 qui commande le fonctionnement des moyens d'impression 19.

Chacun des éléments illustrés en figure 2 est bien connu de l'homme du métier des machines à affranchir possédant un circuit à microprocesseur et, plus généralement, des systèmes de traitement de l'information. Ces éléments ne sont donc pas décrits ici.

La mémoire vive 104 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la suite de la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 104 comporte notamment des registres conservant des informations représentatives du poids de l'objet postal à affranchir, le format de l'objet postal en cours de traitement, le nombre d'objets postaux dans le lot en cours de traitement, des valeurs de compteurs ascendant et descendant qui correspondent à des montants d'affranchissement déjà déposés et restant à déposer avant le rechargement de la machine. Ces derniers registres fonctionnent selon des techniques connues dans le domaine des machines à affranchir (au cours de chaque affranchissement, lorsque le

montant du compteur descendant est supérieur au montant de la marque d'affranchissement à déposer, il est décrémenté du montant de cette marque et le compteur ascendant est incrémenté du même montant).

La mémoire morte 105 est adaptée à conserver le programme de fonctionnement de l'unité centrale de traitement 106, dans un registre " *program1* ", et les données nécessaires au fonctionnement de ce programme ainsi que la table de correspondance mettant en relation des poids, d'une part, à des montants d'affranchissement, d'autre part.

La mémoire morte 105 conserve, en outre, dans un registre "*liste_d'identifiants*", une liste d'identifiants de tâches logicielles autorisées à accéder aux routines qui utilisent des données sensibles (ici des montants d'affranchissement).

En fait, la mémoire dite "morte" 105 est une mémoire réinscriptible qui ne s'efface pas lorsque le dispositif est éteint. Elle n'est réinscriptible que selon des procédures sécurisées et seulement par certaines personnes habilitées, si bien que, pour l'utilisateur quotidien, elle apparaît comme une mémoire morte.

L'unité centrale de traitement 106 est adaptée à mettre en oeuvre le programme conservé en mémoire morte 105, programme dont un algorithme de fonctionnement est illustré en figure 3.

Le programme ou logiciel de la machine à affranchir est un logiciel multitâche, ce qui implique une allocation, par le processeur, d'un espace mémoire, ou pile, associé à chaque tâche. Cet espace mémoire est contenu dans la mémoire vive 104.

Au cours d'une opération 301 :

- la carte électronique 10 est initialisée par l'unité centrale de traitement 106, selon des techniques connues, et

- l'unité centrale de traitement 106 attribue un identifiant (constitué ici d'un numéro) à chaque tâche de l'application.

Au cours d'une opération 302, l'unité centrale 106 exécute une partie de programme ne nécessitant aucun appel à une routine utilisant des données sensibles.

Au cours d'une opération 303, l'unité centrale 106 met en oeuvre une tâche qui fait appel à l'une des routines qui utilisent les données sensibles.

Au cours d'une opération 304, la routine 400 considérée (représentées en traits discontinus) lit l'identifiant de la tâche en cours d'exécution en faisant appel à une routine dite "système" de type connu, destinée à cette lecture.

Ensuite, au cours d'un test 305, la routine 400 compare l'identifiant de la tâche au contenu de la liste d'identifiants conservés en mémoire morte 105 et détermine si cet identifiant de tâche se trouve dans la liste.

Lorsque le résultat du test 305 est positif, la tâche est autorisée à accéder à la routine et l'utilisation de données sensibles est exécutée, au cours d'une opération 306. Puis l'unité centrale 106 retourne au fonctionnement représenté en 302.

Lorsque le résultat du test 305 est négatif, la tâche n'est pas autorisée à accéder à la routine. Le fonctionnement de l'unité centrale 106 est alors arrêtée et une alarme est déclenchée, opération 307, jusqu'à ce que la machine à affranchir soit mise hors tension, opération 308.

On comprend que le procédé de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données visé par la présente invention comporte, mise en oeuvre par ladite routine, une opération 400 de vérification d'identité de chaque tâche logicielle appelant ladite routine.

On comprend aisément que, grâce à l'organisation de la tâche 400, et, en particulier, grâce à la surveillance de l'identité des tâches qui font appel à elle, la modification des données sensibles, par le biais de cette routine est impossible.

En variante, les routines 400 (c'est-à-dire celles qui vérifient l'identité de la tâche les appelant avant d'effectuer un accès à des données sensibles) comportent non seulement les routines qui accèdent aux compteurs de montant d'affranchissement, mais aussi des routines agissant sur des données statistiques ou des paramètres de fonctionnement de la machine à affranchir.

Dans le mode de réalisation décrit et représenté, ladite opération de vérification 400 comporte une opération de lecture d'un identifiant de ladite

tâche 304 et une opération de comparaison 305 dudit identifiant, d'une part, et d'identifiants prédéterminés, d'autre part.

Dans le mode de réalisation décrit et représenté, chaque routine agissant sur les données sensibles met en oeuvre ladite opération de vérification 400.

Le dispositif de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données, caractérisé en ce qu'il comporte, comme moyen de vérification l'unité centrale 106, associée aux mémoires 104 et 105, pour vérifier l'identité de chaque tâche logicielle appelant ladite routine, ce moyen de vérification étant mis en oeuvre par ladite routine.

REVENDICATIONS

1. Procédé de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données, caractérisé en ce qu'il comporte, mise en oeuvre par ladite routine, une opération de vérification d'identité de chaque tâche logicielle appelant ladite routine (400).

2. Procédé de protection selon la revendication 1, caractérisé en ce que ladite opération de vérification (400) comporte une opération de lecture d'un identifiant de ladite tâche (304) et une opération de comparaison (305) dudit identifiant, d'une part, et d'identifiants prédéterminés, d'autre part.

3. Procédé de protection selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que chaque routine agissant sur lesdites données met en oeuvre ladite opération de vérification (400).

4. Dispositif de protection de données sensibles contre l'usage d'une routine agissant sur lesdites données, caractérisé en ce qu'il comporte un moyen de vérification (104, 105, 106) adapté à vérifier l'identité de chaque tâche logicielle appelant ladite routine, le moyen de vérification étant mis en oeuvre par ladite routine.

5. Dispositif de protection selon la revendication 4, caractérisé en ce que ledit moyen de vérification (104, 105, 106) comporte un moyen de lecture (104, 105, 106) d'un identifiant de ladite tâche et un moyen de comparaison (104, 105, 106) dudit identifiant, d'une part, et d'identifiants prédéterminés, d'autre part.

6. Procédé de protection selon l'une quelconque des revendications 4 ou 5, caractérisé en ce que chaque routine agissant sur lesdites données met en oeuvre ledit moyen de vérification (104, 105, 106).

7. Machine à affranchir (1), caractérisée en ce qu'elle comporte un dispositif selon l'une quelconque des revendications 4 à 6.

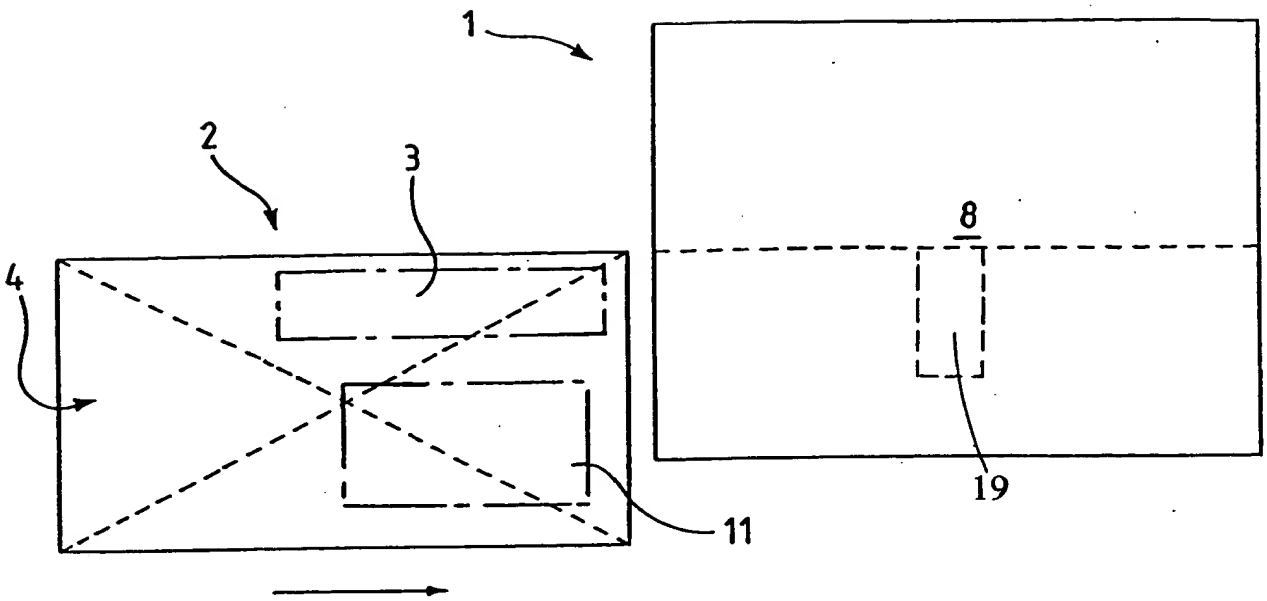

Fig. 1A

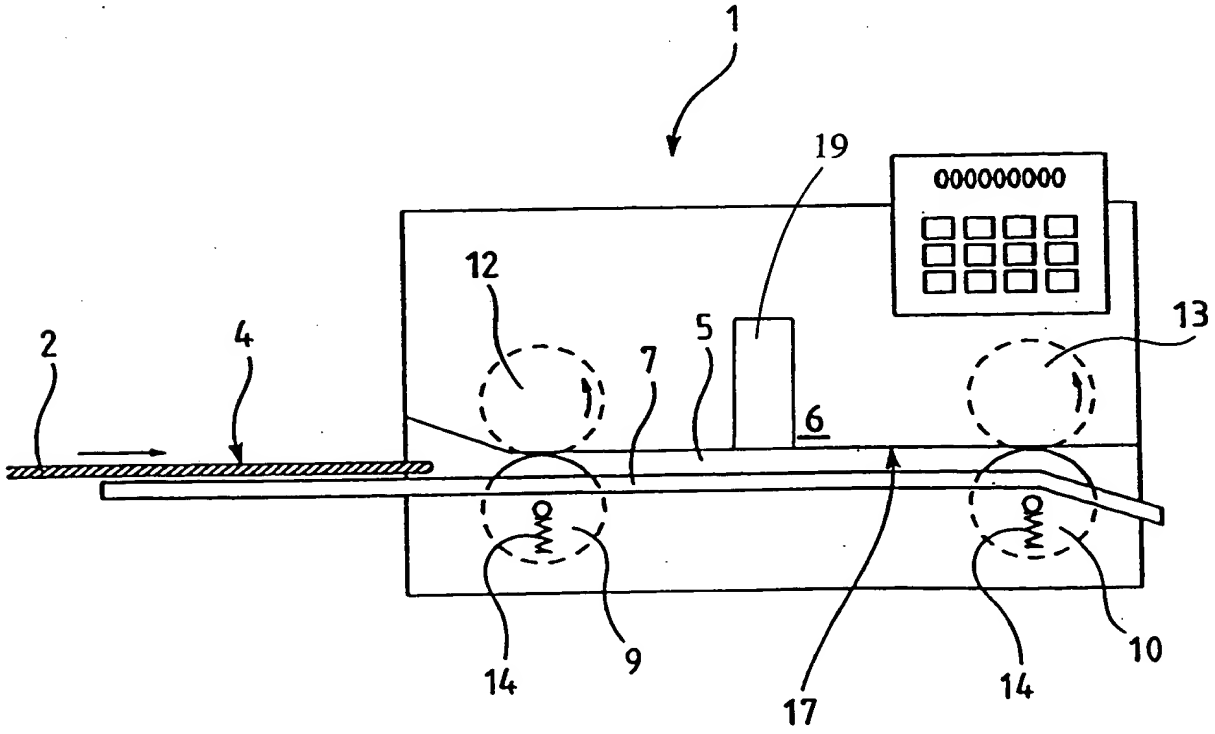

Fig. 1B

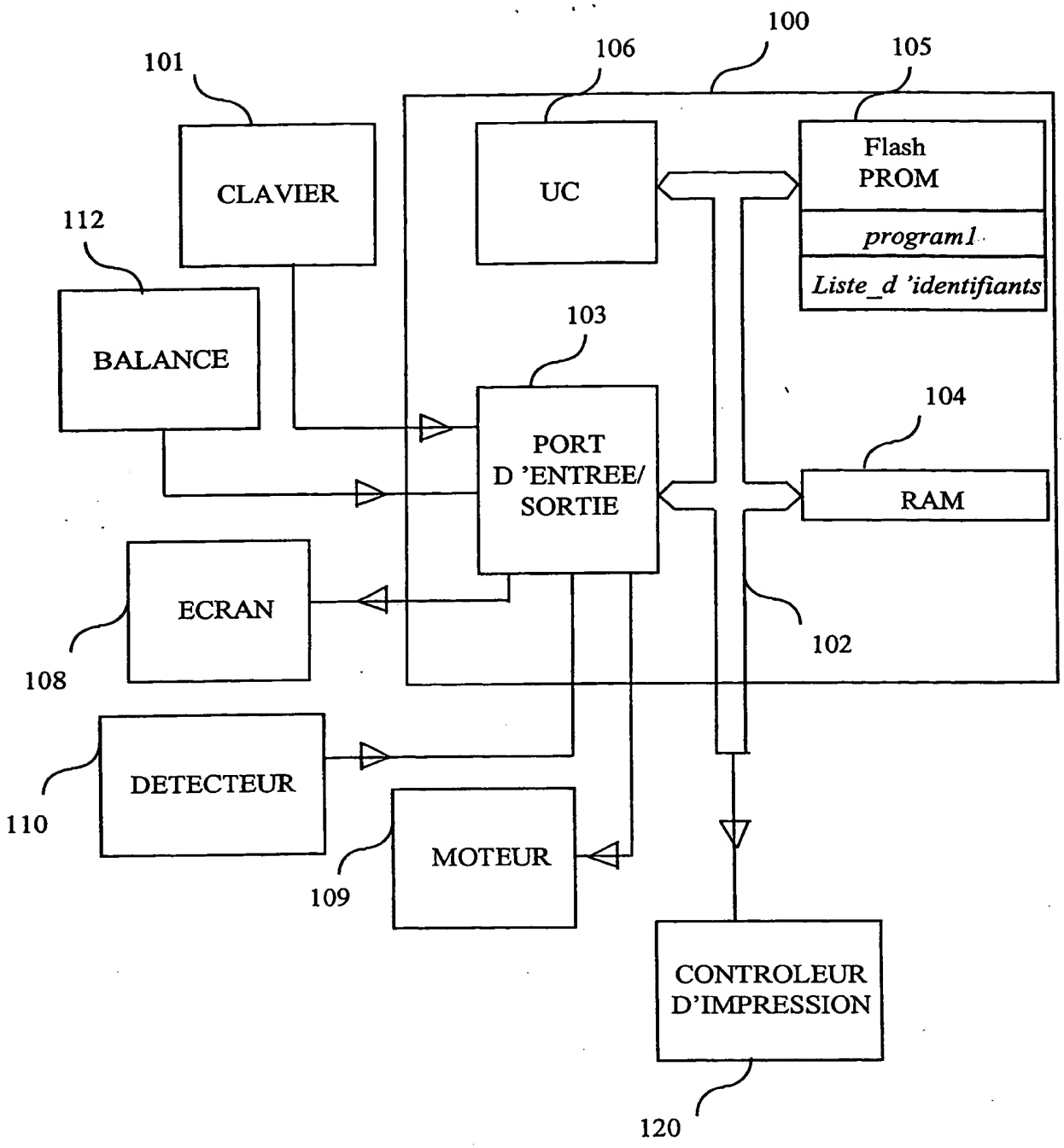
100
101
106
105
CLAVIER
UC
Flash
PROM
program1
Liste_d 'identifiants
112
BALANCE
103
104
PORT
D 'ENTREE/
SORTIE
RAM
ECRAN
102
108
DETECTEUR
110
MOTEUR
109
CONTROLEUR
D'IMPRESSION
120

Fig. 2

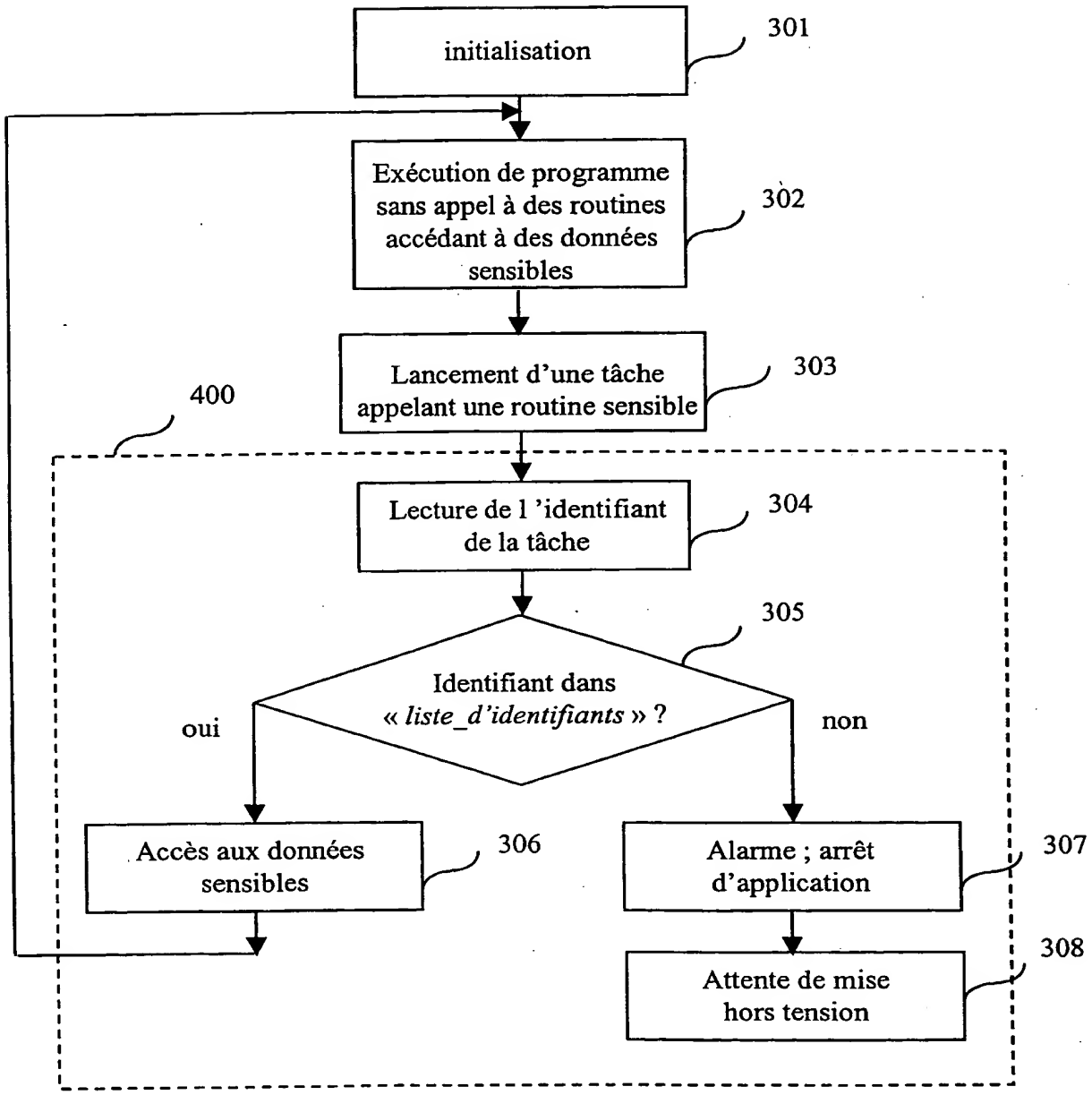
initialisation
301
Exécution de programme sans appel à des routines accédant à des données sensibles
302
Lancement d'une tâche appelant une routine sensible
303
400
Lecture de l 'identifiant de la tâche
304
305
Identifiant dans « liste_d'identifiants » ?
oui
non
Accès aux données sensibles
306
Alarme ; arrêt d'application
307
Attente de mise hors tension
308

Fig.3